DataTraveler Vault and DataTraveler Vault – Privacy Edition

Advanced Security and High Performance White Paper

A leading-edge solution for business and corporate IT users that combines advanced data security with outstanding performance.

Assembled in the USA
TAA Compliant

Introduction

Conveniently small, portable, and easy to use, USB Flash drives have become one of the fastest-growing Flash memory products. Many business customers and advanced consumers require key features to enhance their use of USB Flash drives, including advanced security, and high performance without sacrificing ease of use.

Kingston's DataTraveler® Vault ("DT Vault" or simply "DTV") and DataTraveler Vault – Privacy Edition ("DT Vault – Privacy" or simply "DTVP") USB Flash drives meet these needs. With the industry's highest performance and two-layer security incorporating hardware-based 256-bit AES encryption, DTV and DTVP drives are among the most secure USB Flash drives for Windows® -based systems in the world.

For government agencies and enterprises looking for Trade Agreement Act (TAA) compliant products, the DTV and DTVP are assembled in the USA.

This white paper will provide more details on the advanced security and high-performance features of the DTV and DTVP ultra-secure USB storage drives.

1.0 DT Vault and DT Vault – Privacy Edition Security Features

Robust security is the primary feature that was engineered into the DTV and DTVP drives. A two-layer security mechanism that features user authentication and hardware-based, real-time data encryption guards sensitive data stored in the privacy zone.

Both drives incorporate a built-in encryption/decryption co-processor for advanced security. They feature an industry-leading, high-performance Flash memory controller that offers one of the highest levels of USB 2.0 performance available on the market today.

The major difference between the DTV and DTVP drives is that the DTV drive allows for a public zone where files are always visible and accessible. The DTV – Privacy Edition drive does not allow a public zone; all data is invisible and encrypted until the user has successfully entered a valid password to access the privacy zone and its files. In addition, DTVP drives enforce a complex password, with a minimum length of 6 characters and requiring a mix of three of the following: Upper/Lower-Case Alphabetic, numeric, and special characters. Complex passwords, coupled with limited password retry capabilities (explained in section 1.2), make DTVP drives ultra-secure for enterprise-grade data protection.

1.1 User Authentication

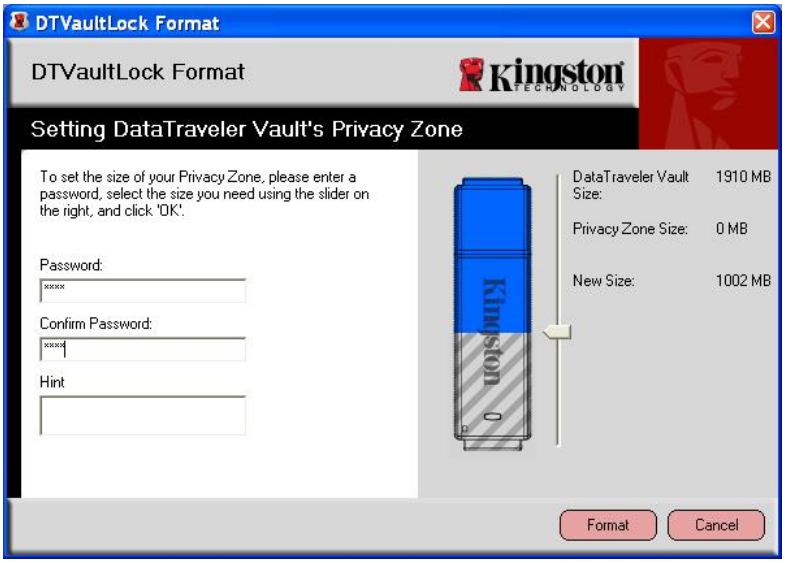
To activate the security features of the DataTraveler Vault, the user must create a privacy or encrypted zone. As shipped from the factory, the DT Vault drive is set up as a single, public zone. All data stored in the public zone can be read by any host computer.

DTVP drives do not allow a public zone and are set up with a 100 percent privacy zone. There is no way to set up a public zone for data security reasons. In addition, DTVP drives do not provide a DTVaultLock program – they auto-launch their built-in login program to enter a password and access the drive.

1.2 Public and Privacy Zones on the DT Vault and DT Vault - Privacy Edition Drives

The owner of the DT Vault creates a privacy zone for the storage of secure data using DTVaultLock, the DT Vault's access protection software for Windows-based systems. He or she defines a password to control access to the privacy zone, which is an area on the drive in which all sensitive data is kept. This password is stored in the DT Vault in an encrypted mode that makes it very difficult to decrypt.

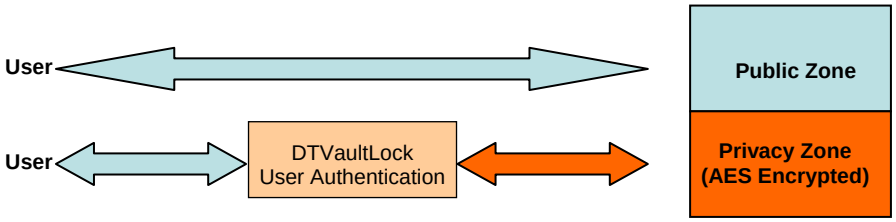
The public and private zones are set when the DT Vault drive is first used, or when the owner wants to update the relative sizes, through the DTVaultLock program as shown below:



DTV features a DTVaultLock Console to set zone sizes, public and private partitions

Once a privacy zone is created using the DTVaultLock console, data stored there will be encrypted using the Advanced Encryption Standard (AES-256).

Without a valid password, unauthorized access to the privacy zone is blocked, and the data remains encrypted and protected. Whenever the DT Vault is connected to a host computer, the DTVaultLock console needs to be used to log into and access the privacy zone:



The privacy zone can only be accessed after valid password logon

Unlike other software consoles that allow unlimited numbers of incorrect passwords, DT Vault has a factory-set limit that locks the privacy zone after 10 *consecutive* failed attempts to log in. This limit blocks "Brute Force Attacks," in which programs are used to test millions of password combinations to find the correct password. After 10 consecutive invalid attempts, the DT Vault will lock out the privacy zone; the only option left at this point is to reformat the drive, destroy the encryption key, thus losing all the encrypted data stored in the privacy zone.

DTVP drives only allow a privacy zone so there is no option to create a public zone. When a user successfully enters a valid password, the privacy zone allows access to all the files stored there. Like DTV, the DTVP also locks the privacy zone after 10 consecutive failed attempts to log in.

2.0 Hardware-Based, Real-Time Data Encryption

Cryptography is the science of encrypting and decrypting data using a special "key" to encode and decode the data. Unencrypted data (or files) are processed through an encryption engine (either in software or in hardware) to produce an encrypted file; without the exact key, the data is unusable.

Kingston DT Vault and DT Vault – Privacy Edition drives feature one of the industry's best, most robust data encryption capabilities. Their encryption technology is based upon the same standard used in high-security applications – the Advanced Encryption Standard (AES). Keys are sequences of bits (256 in the case of AES-256) which are used by the encryption/decryption engine to uniquely process the data.

2.1 Advanced Encryption Standard (AES-256)

The Advanced Encryption Standard was defined by the National Institute of Standards and Technology (NIST) in 1997. Kingston has adopted the AES-256 standard for 256-bit encryption/decryption. With this standard, if a key is used to encrypt data, the exact same key must be used to decrypt the data. Without the same key, data would be a useless string of data.

2.2 DT Vault and DT Vault – Privacy Edition's Real-Time, Hardware-Based Encryption

The AES encryption/decryption functions are performed directly in the DTV's or DTVP's Flash memory controller. When a DTV or DTVP drive is connected to a host computer, data and file management commands are exchanged between the host computer and the DTV/DTVP Flash memory and USB controller.

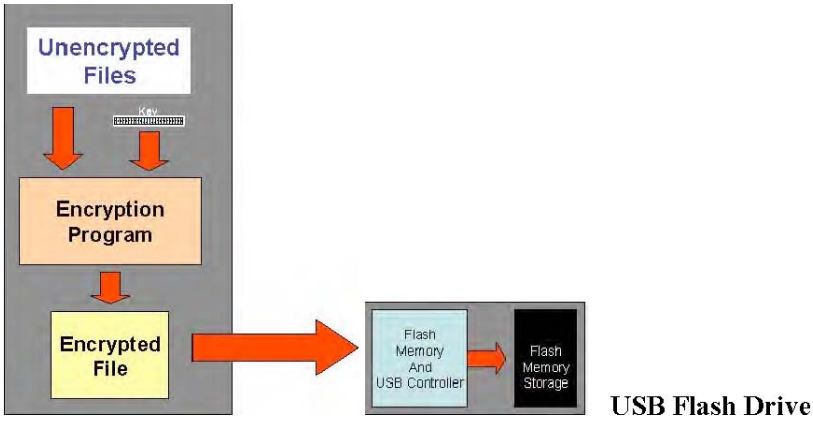
With DT Vault drives, when data is written to a public zone, the data is written to the Flash memory storage without any encryption. This data can be read on any host computer or other device. To access the privacy zone, the user is required to use the DTVaultLock console and enter a valid password. Once logged in, the host computer will be able to write and read data from the privacy zone.

With DT Vault – Privacy Edition drives, a Login program is automatically launched to allow for the entry of a valid password. Once the password is successfully entered, the data content of the drive is visible and accessible.

When data is written to a privacy zone of either the DT Vault or the DT Vault – Privacy Edition, it is encrypted by the AES Encryption and Decryption Co-Processor in real-time, and then written to the Flash memory storage. Similarly for reads, the data is decrypted real-time on the DT Vault drive and then sent to the host computer.

Without the unique 256-bit key, which is uniquely generated for the DT Vault utilizing a true random number generator, encrypted data is nearly impossible to decode.

3.0 Software-Based Encryption Host Computer



Software-Based Encryption

In this case, the user has to explicitly run a program to encrypt a file. When the file is encrypted, the file can then be copied to the USB Flash drive.

When run on host computers, encryption and decryption programs take up a lot of processor resources and reduce overall system performance.

3.1 DT Vault & DT Vault – Privacy Edition Hardware-Based Encryption

Because the processor-intense AES encryption/decryption is done through a DTV's or DTVP's dedicated Co-Processor, both drives offer an industry-leading performance level over software encryption programs.

In addition, utilizing hardware encryption on both drives does not expose the AES "key" to host computers or networks, further increasing security. The encrypted user password and the key are never shared outside of the DT Vault or DT Vault – Privacy Edition drives. With software-based encryption approaches, the key or keys are exposed to the host computer and network.

There is no performance penalty when storing files on the public and privacy zones in a DT Vault or DT Vault – Privacy Edition.

Benefits of DTV/DTVP Hardware-Based Encryption vs. Software Approaches

	DTV & DTVP with built-in, hardware-based encryption/decryption	Other USB Drives with Software-based Encryption
Invalid Password Retry limit	Yes	Rare
Advanced hashing (encoding) of user password to secure it	Yes	Varies
Dedicated AES co-processor on USB drive	Yes	No
Data encrypted/decrypted on host computer	No	Yes
AES key exposed to host computer or network	No	Yes
Performance penalty	No	Yes (40-50% slower)
Transparent encryption/decryption (drag & drop; copy and paste files)	Yes	Rare

4.0 Certifications and Operating System Support:

The Kingston DT Vault and DT Vault — Privacy Edition are certified as Hi-Speed USB 2.0 drives. OS support, especially of encryption features, is shown below:

Operating System	DTVP	DTV
Windows compatibility	Vista; 2000 SP3, 4; XP SP1, 2	Vista; 2000 SP4; XP SP1, 2
Mac OS 10.3.x and above / Linux Kernel 2.6 and above	No	Yes (file transfer only in public zone)

The DT Vault and DT Vault – Privacy Edition drives also meet the provisions of the Cryptography Note (Note 3) in Category 5, Part 2, of the Commerce Control List (United States Department of Commerce – Bureau of Industry and Security – Encryption regulatory).

5.0 DataTraveler Vault & DataTraveler Vault - Privacy Edition Performance*

Kingston's DTV and DTVP USB Flash drives are engineered with a state-of-the-art, Hi-Speed USB 2.0 controller that delivers outstanding performance. Even when AES-256 encryption/decryption security is used, their performance is not reduced due to the built-in AES-256 co-processor. DT Vault and DT Vault – Privacy Edition drives makes no performance compromises while delivering an advanced level of security.

*Speed may vary due to host hardware, software and usage. Based on internal tests.

Kingston DataTraveler Transfer Rates and Security Features

	Read Rate (Peak)*	Write Rate (Peak)*	Public/Privacy Zone Support	Advanced Security
DataTraveler Vault	24 MB/sec.	10 MB/sec.	Yes	Yes (Hardware AES-256)
DataTraveler Vault – Privacy Edition	24 MB/sec.	10 MB/sec.	No – Only Privacy Zone	Yes (Hardware AES-256)
DataTraveler 400	15 MB/sec.	7 MB/sec.	Yes	No
DataTraveler II	11 MB/sec.	7 MB/sec.	Yes	No
DataTraveler	5 MB/sec	1.5 MB/sec.	No	No

*Speed may vary due to host hardware, software and usage. Based on internal tests.

5.1 Hi-Speed USB 2.0 Interface and Waterproof protection

Because the USB Hi-Speed standard is a range (for more information, please see Kingston's Flash Memory Guide at www.kingston.com/products/pdf_files/FlashMemGuide.pdf), products can offer different performance levels despite having the same Hi-Speed USB logo. Kingston's DataTravelers all feature advanced Flash controllers and deliver outstanding performance.

The DT Vault and DT Vault – Privacy Edition drives offer data transfer rates of up to 24 MB/sec. read and 10 MB/sec. write (15 MB/sec. read speed for 1GB capacity). Even with encryption, their performance levels are not significantly impacted due to the real-time, hardware-based encryption/decryption technology built into the drives.

For added protection, the drives are designed to withstand harsh operating conditions, and feature waterproof industrial aluminum casings. The drives are waterproof rated, conforming to the International Electrotechnical Commission (IEC) 60529 IPX8 standards to protect against water damage – even if they're submerged in depths up to 4 feet. The device must be clean and dry before using.

6.0 Conclusion

Kingston's DataTraveler Vault and DataTraveler Vault – Privacy Edition drives are state-of-the-art, advanced security, high-performance Flash drives. They are ideally suited for business organizations and government agencies as well as advanced consumers seeking the advanced security of hardware AES encryption and high-performance USB 2.0 interface.

© 2008 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708. USA. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Printed in the USA.